UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

ELLYSE WISSEL; MICHELLE ANDERSON; and MCLAIN MOTT, individually and on behalf of all others similarly situated, Plaintiffs, v. RURAL MEDIA GROUP, INC., Defendant.	Civil Action No. 4:24-cv-999 **COMPLAINT - CLASS ACTION** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

INTRODUCTION

Ellyse Wissel ("Plaintiff Wissel"), Michelle Anderson ("Plaintiff Anderson"), and McLain Mott ("Plaintiff Mott") (collectively, "Plaintiffs") individually and on behalf of all others similarly situated, make the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to themselves or their counsel, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiffs bring this action to redress Defendant Rural Media Group, Inc.'s ("Defendant") practice of knowingly disclosing Plaintiffs' and its other customers' identities and the identities of the prerecorded video materials to which they purchased access on Defendant's www.cowboychannelplus.com website (the "Website") to third parties in violation of the federal Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710.

2. Over the past two years, Defendant has systematically transmitted (and continues to transmit today) its customers' personally identifying video viewing information to at least three companies using snippets of code called tracking pixels.

3. Defendant knowingly and intentionally transmitted this personally identifying video viewing information to: (i) Meta Platforms, Inc. ("Meta"), formerly known as Facebook, Inc. ("Facebook"); (ii) Alphabet, Inc., formerly known as Google ("Google"); and Yahoo! Inc. ("Yahoo").

4. In the simplest terms, the tracking pixels installed by Defendant capture and disclose to their respective third parties information that reveals the specific videos that a particular person watched through a paid subscription on Defendant's Website (hereinafter, "Private Viewing Information").

5. Defendant disclosed and continues to disclose its customers' Private Viewing Information to these third parties without asking for, let alone obtaining, its customers' consent to these practices.

6. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), damages in the amount of $2,500.00, *see id.* § 2710(c).

7. Accordingly, on behalf of themselves and the putative Class members defined below, Plaintiffs bring this Class Action Complaint against Defendant for intentionally and unlawfully disclosing their Private Viewing Information to third parties.

PARTIES

I. Plaintiff Ellyse Wissel

8. Plaintiff Wissel is, and at all times relevant hereto was, a citizen and resident of Denton County, Texas.

9. Plaintiff Wissel has used and continues to use the same device to maintain and access an active Facebook account throughout the relevant period in this case.

10. Plaintiff Wissel has purchased an annual subscription to Defendant's Website which provides access to prerecorded video materials. Plaintiff Wissel provided her name, email address, and home address in association with the purchase of this subscription. Plaintiff Wissel has watched prerecorded video materials on Defendant's Website during the time frame applicable to this case using her paid subscription. Accordingly, Plaintiff Wissel requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its Website.

11. At all times relevant hereto, including when purchasing subscription access to prerecorded video material from Defendant on its Website, Plaintiff Wissel had a Meta account, a Meta profile, and an FID associated with such profile.

12. Plaintiff Wissel has watched prerecorded videos on Defendant's Website through her paid subscription while logged into Facebook during the last two years.

13. When Plaintiff Wissel purchased a subscription from Defendant, Defendant disclosed to Meta Plaintiff's FID coupled with a URL identifying the subscription she purchased, among other information about Plaintiff Wissel and the device she used to make the purchase.

14. When Plaintiff Wissel viewed prerecorded videos on the Website through the use of that subscription, Defendant disclosed to Meta Plaintiff's FID coupled with the specific URL identifying the video she watched, including a unique identifying

code which correlating to that video, among other information about Plaintiff Wissel and the device she used to watch the video.

15. Plaintiff Wissel has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Viewing Information to Meta.

16. Because Defendant disclosed Plaintiff Wissel's Private Viewing Information (including her FID, the fact that she purchased a subscription, the identity of the prerecorded video material she viewed through her subscription, and the URL where such video is available for viewing) to Meta during the applicable statutory period, Defendant violated Plaintiff Wissel's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

II. Plaintiff Michelle Anderson

17. Plaintiff Anderson is, and at all times relevant hereto was, a citizen and resident of Okeechobee County, Florida.

18. Plaintiff Anderson has used and continues to use the same device to maintain and access an active Facebook account throughout the relevant period in this case.

19. Plaintiff Anderson has purchased a monthly subscription to Defendant's Website which provides access to prerecorded video materials. Plaintiff Anderson provided her name, email address, and home address in association with the purchase of this subscription. Plaintiff Anderson has watched prerecorded video materials on

Defendant's Website during the time frame applicable to this case using her paid subscription. Accordingly, Plaintiff Anderson requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its Website.

20. At all times relevant hereto, including when purchasing subscription access to prerecorded video material from Defendant on its Website, Plaintiff Anderson had a Meta account, a Meta profile, and an FID associated with such profile.

21. Plaintiff Anderson has watched prerecorded videos on Defendant's Website through her paid subscription while logged into Facebook during the last two years.

22. When Plaintiff Anderson purchased a subscription from Defendant, Defendant disclosed to Meta Plaintiff's FID coupled with a URL identifying the subscription she purchased, among other information about Plaintiff Anderson and the device she used to make the purchase.

23. When Plaintiff Anderson viewed prerecorded videos on the Website through the use of that subscription, Defendant disclosed to Meta Plaintiff's FID coupled with the specific URL identifying the video she watched, including a unique identifying code which correlating to that video, among other information about Plaintiff Anderson and the device she used to watch the video.

24. Plaintiff Anderson has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Viewing Information to Meta.

25. Because Defendant disclosed Plaintiff Anderson's Private Viewing

Information (including her FID, the fact that she purchased a subscription, the identity of the prerecorded video material she viewed through her subscription, and the URL where such video is available for viewing) to Meta during the applicable statutory period, Defendant violated Plaintiff Anderson's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

III. Plaintiff McLain Mott

26. Plaintiff Mott is, and at all times relevant hereto was, a citizen and resident of Pima County, Arizona.

27. Plaintiff Mott has used and continues to use the same device to maintain and access an active Facebook account throughout the relevant period in this case.

28. Plaintiff Mott has purchased a subscription to Defendant's Website which provides access to prerecorded video materials. Plaintiff Mott provided his name, email address, and home address in association with the purchase of this subscription. Plaintiff Mott has watched prerecorded video materials on Defendant's Website during the time frame applicable to this case using his paid subscription. Accordingly, Plaintiff Mott requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its Website.

29. At all times relevant hereto, including when purchasing subscription access to prerecorded video material from Defendant on its Website, Plaintiff Mott had a Meta account, a Meta profile, and an FID associated with such profile.

30. Plaintiff Mott has watched prerecorded videos on Defendant's Website through his paid subscription while logged into Facebook during the last two years.

31. When Plaintiff Mott purchased a subscription from Defendant, Defendant disclosed to Meta Plaintiff's FID coupled with a URL identifying the subscription he purchased, among other information about Plaintiff Mott and the device he used to make the purchase.

32. When Plaintiff Mott viewed prerecorded videos on the Website through the use of that subscription, Defendant disclosed to Meta Plaintiff's FID coupled with the specific URL identifying the video he watched, including a unique identifying code which correlating to that video, among other information about Plaintiff Mott and the device he used to watch the video.

33. Plaintiff Mott has never consented, agreed, authorized, or otherwise permitted Defendant to disclose his Private Viewing Information to Meta.

34. Because Defendant disclosed Plaintiff Mott's Private Viewing Information (including his FID, the fact that he purchased a subscription, the identity of the prerecorded video material he viewed through his subscription, and the URL where such video is available for viewing) to Meta during the applicable statutory period, Defendant violated Plaintiff Mott's rights under the VPPA and invaded his statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

IV. Defendant Rural Media Group, Inc.

35. Defendant Rural Media Group, Inc. is a Delaware limited liability company with a principal place of business at 17455 Arbor Street, Omaha, Nebraska 68130.

36. Defendant operates the Website www.cowboychannelplus.com, which is a steaming video service providing access to a variety of Western-themed prerecorded video programming.

37. Defendant conducts business within the jurisdictional boundaries of this district, is registered to do business in the State of Texas, and may be served process through its registered agent, C T Corporation System, at the address 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

38. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

39. Personal jurisdiction and venue are proper in this district because of a forum-selection clause in the Terms of Service governing Defendant's and Plaintiffs' use of the Website which provides that "Each party to this Agreement hereby submits to the exclusive jurisdiction of the state and federal courts sitting in the County of Tarrant in the State of Texas, and waives any jurisdictional, venue or inconvenient forum objections to such courts."

VIDEO PRIVACY PROTECTION ACT

40. The VPPA prohibits companies (like Defendant) from knowingly disclosing to third parties (like Meta, Google, and Yahoo) information that personally identifies consumers (like Plaintiffs and the putative class members) as having requested or obtained particular videos or other audio-visual materials.

41. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4). It defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

42. Leading up to the VPPA's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sen. Simon). Senators at the time were particularly troubled by disclosures of records that reveal

consumers' purchases and rentals of videos and other audiovisual materials because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." *Id*. at 8 (statement of Sen. Leahy).

43. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, the personal nature of such information, and the need to protect it from disclosure, is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id*.

44. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a more recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right

to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[1]

45. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[2]

46. In this case, however, Defendant deprived Plaintiffs and numerous other similarly situated persons of that right by systematically (and surreptitiously) disclosing their Private Viewing Information to Meta, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

47. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything

[1] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury.

[2] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, franken.senate.gov (Jan. 31, 2012).

we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[3]

48. Over two decades later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a 26 billion dollar per year online advertising industry in the United States.[4]

49. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[5]

50. In fact, an entire industry exists where companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[6]

---

[3] Transcript, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[4] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), available at https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[5] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

[6] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), available at http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/ .

51. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[7]

52. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[8]

53. Recognizing the severe threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[9]

---

[7] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), available at https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html#:~:text=It's%20called%20the%20Acxiom%20Corporation,to%20know%20much%2C%20much%20more.

[8] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. On Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) available at https://www.commerce.senate.gov/services/files/3bb94703-5ac8-4157-a97b-%20a658c3c3061c.

[9] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012),

54. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like Defendant share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[10]

55. Disclosures like Defendant's are particularly dangerous to the elderly. The FTC notes that "[t]he elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[11]

56. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like Defendant's are particularly troublesome because of their cascading nature: "Once

---

available at https://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

[10] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.

[11] Prepared Statement of the FTC on "Fraud Against Seniors" before the Special Committee on Aging, United States Senate (August 10, 2000).

marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[12]

57. Defendant is not alone in violating its customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

II. Consumers Place Monetary Value on Their Privacy and Consider Privacy Practices When Making Purchases

58. As the data aggregation industry has grown, so has consumer concerns regarding personal information.

59. A survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do protect their privacy online.[13] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[14]

---

[12] *Id*.

[13] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

[14] *Id*.

60. Thus, as consumer privacy concerns grow, consumers increasingly incorporate privacy concerns and values into their purchasing decisions, and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[15]

61. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[16]

62. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[17]

---

[15] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), available at https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[16] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on Monetizing Privacy* (Feb. 27, 2012), available at https://www.enisa.europa.eu/publications/monetising-privacy.

[17] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

As such, where a business offers customers a product or service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a product or service of less value than the product or service paid for.

III. Defendant is a Video Tape Service Provider

63. Defendant sells access to prerecorded video materials to consumers on the Website (www.cowboychannelplus.com).

64. These materials include thousands of hours of prerecorded videos. Among these videos are recordings of numerous rodeo athletic competitions, including Professional Rodeo Cowboys Association competitions and its championship event, the National Finals Rodeo. Other prerecorded video content available through a subscription to the Website includes western sports news programs, equine sports programs, and western lifestyle programs.[18]

65. The prerecorded videos available on Defendant's website are only available to paying subscribers.

66. Defendant offers multiple paid subscription tiers to the Website, include an annual subscription for $119.99 and a monthly subscription for $9.99.

67. To buy a subscription providing access to the prerecorded video materials on Defendant's Website, a person must provide at least his or her name,

[18] *See* Rural Media Group, Inc., "Welcome – Cowboy Channel+," available at https://www.cowboychannelplus.com/.

email address, billing address, and credit or debit card (or other form of payment) information.

IV. Defendant Uses Tracking Pixels to Systematically Disclose its Customers' Private Viewing Information to Meta, Google, and Yahoo

68. A tracking pixel is a piece of JavaScript code added to a website as a graphic element that is loaded when a user arrives at the website hosting the pixel.

69. When a user visits a website which has tracking pixels enable, an instance of the tracking pixel loads in the HTML code of the page on the user's web browser.

70. Sometimes, a cookie corresponding to the tracking pixel already exists in the browser. In those cases, the cookie contains a unique ID that follows the user of the internet browser from web page to web page and that cookie connects with the tracking pixel.

71. In other cases, a cookie corresponding to the cookie does not exist on the browser. In those cases, a unique ID is created and saved in a cookie.

72. After identifying the corresponding cookie (with its unique ID), the tracking pixel's embedded URL points to a third party's (e.g. Meta, Google, Yahoo) designated tracking URL and reports to the third party the user's activity for the duration of the visit, along with the unique ID stored in the cookie which identifies the specific web user.

73. To implement a tracking pixel, a website administrator must place the base tracking pixel code in the website's JavaScript code. That code acts an initiator for the tracking pixel's behavior. Once initiated, the code will load a library of functions (e.g., fbevents.js for the Meta Pixel; analystics.js, gtag.js, gtm.js and/or optimize.js for Google Analytics; and ytc.js for the Yahoo Dot) that enable to pixel to respond to certain actions taken by the user of the internet browser and initiate data transmissions regarding the user (e.g., sending querystring parameters and cookie values) to the third-party's tracking URL.

74. Defendant has installed and programed tracking pixels from at least Meta, Google, and Yahoo on the Website and uses these pixels to transmit the Private Viewing Information of its subscribers to those third parties in violation of the VPPA.

A. The Meta Pixel

75. Defendant has disclosed the identities and Private Viewing Information of its subscribers to Meta using a snippet of programming code called the "Meta Pixel," which Defendant installed and configured on the Website.

76. The information Defendant disclosed (and continues to disclose) to Meta via the Meta Pixel includes the customer's Facebook ID ("FID") and the identity of the specific prerecorded video material that each of its customers watched through a subscription to its Website.

77. An FID is a unique sequence of numbers linked to a specific Meta profile. A Meta profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person, such as their photographs, contact information, employer, etc.).

78. Entering "Facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name, but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. When someone has access to an individual's FID, they are able to precisely identify that individual person.

79. As alleged below, whenever a person with a Meta account views prerecorded video material on Defendant's Website through that person's paid subscription, the Meta Pixel technology that Defendant intentionally installed on its Website transmits the customer's personally identifying information and detailed Private Viewing Information (revealing the specific identity of the prerecorded video material that he or she purchased) to Meta – all without the customer's consent, and in clear violation of the VPPA.

80. The Meta Pixel technology also reveals that a consumer has purchased a subscription to access prerecorded video content on Defendant's website alongside that consumer's personally identifying information.

81. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta."[19] Meta is now the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

82. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to monitor and track the actions taken by visitors to their websites and to report them back to Meta. This allows companies like Defendant, Meta, and third-party marketing companies to build detailed profiles about websites' customers and serve them with highly targeted advertising.

83. Additionally, a Meta Pixel installed on a company's website allows Meta to "match [] website visitors to their respective Facebook User accounts."[20] This is because Meta has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[21] – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter*

[19] *See* Facebook, "Company Info," available at https://about.fb.com/company-info./.

[20] Meta, "Get Started – Meta Pixel," available at https://developers.facebook.com/docs/meta-pixel/get-started/.

[21] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

alia, the FID of the website's visitor. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

84. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

85. Simply put, if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are then able to "track [] the people and type of actions they take,"[22] including, as relevant here, the specific prerecorded video material that they purchase or view on the website.

86. Defendant knowingly uses the Meta Pixel to transmit the Private Viewing Information of its customers to Meta.

87. Whenever a person with a Meta account purchases a subscription to view prerecorded video materials on the Website, Defendant uses – and has used at all

[22] Meta, "Retargeting: How to Advertise to Existing Customers with Ads on Facebook," available at https://www.facebook.com/business/goals/retargeting?checkpoint_src=any.

times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the person who made the purchase as well as the fact that the person is purchasing requesting or obtaining video material from Defendant. That is because the Meta Pixel transits the individual's FID and the URL of each page in the check-out flow to Facebook, meaning that their identity and each stage of the purchasing process is transmitted to Facebook.

88. Furthermore, whenever a person with a Meta account logs into his or her account on Defendant's Website (obtained through purchasing a subscription) and watches a prerecorded video, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the person who watched the video, the URL of the webpage containing the video, a publicly-available unique identifier associated with the video, and the name of the video.

89. Each watchable video on Defendant's website is hosted on one dedicated webpage where it is the only playable video on that page.

90. The URL of each webpage containing a prerecorded video on Defendant's Website is sufficient to identify the video on that page.

91. The name of the video hosted on any individual webpage available on Defendant's Website is sufficient to identify that video.

92. Furthermore, each video hosted on Defendant's Website is assigned a unique numerical identifier. This unique numerical identifier is accessible to subscribers and non-subscribers to the Website alike. Each video on Defendant's

website is hosted on a webpage with a URL which incorporates the unique numerical identifier of that video.

93. Thus, when a subscriber who is logged into Facebook on their device clicks a link to any page hosting a video on Defendant's website (and thereby requests and obtains access to that video), Defendant transmits that subscriber's personally identifying FID, the URL of the webpage hosting the video, the name of the video, and the publicly available unique numerical identifier of the video to Facebook through the operation of the Meta Pixel.

94. In these ways, among other methods, Defendant knowingly discloses to Meta the Private Viewing Information of its consumers.[23]

95. Each of the Plaintiffs have purchased a subscription to Defendant's Website while logged into Facebook during the last two years. Accordingly, Defendant has transmitted each of the Plaintiffs' identities and the fact that they requested or obtained a subscription providing access to prerecorded video material to Meta during the last two years.

96. Each of the Plaintiffs have watched a prerecorded video on Defendant's Website through their paid subscription while logged into Facebook

[23] Specifically, when a consumer requests and obtains access to a prerecorded video on Defendant's Website, the Website executes a GET request to Facebook's tracking URL "https://www.facebook.com/tr" and sends it querystring parameters and cookie values which disclose the unique numerical identifier of the video, the URL of the webpage hosting the video, and the consumer's FID.

during the last two years. Accordingly, Defendant transmitted each of the Plaintiffs' identities, the identities of the videos they requested and obtained access to, and the URLs of the webpages hosting those videos to Meta during the last two years.

97. Defendant intentionally programmed its Website to include the Meta Pixel code in order to take advantage of the targeted advertising and other informational and analytical services offered by Meta.

98. The Meta Pixel code systematically transmits to Meta the FID of each person with a Meta account who watches prerecorded video material on its Website, along with the specific identity of the prerecorded video material that the person requested or obtained.

99. The Meta Pixel code systematically transmits to Meta the FID of each person with a Meta account who purchases a subscription to prerecorded video material on its Website, along with fact that the person purchased a paid subscription.

100. With only a person's FID and the identity of the prerecorded video material requested or obtained (or URL where such material is available)—all of which Defendant knowingly provides to Meta on a systematic basis—any ordinary person could learn the identity of the person to whom the FID corresponds and identify the specific prerecorded video material that the person requested and obtained. The person's identity can be determined by simply by accessing the URL www.facebook.com/[*insert the person's FID here*]/.

101. With only a person's FID and the fact that the person purchased a subscription to the Defendant's Website—all of which Defendant knowingly provides to Meta on a systematic basis—any ordinary person could learn the identity of the person to whom the FID corresponds and identify the prerecorded video materials that the person requested and obtained. The person's identity can be determined by simply by accessing the URL www.facebook.com/[*insert the person's FID here*]/.

102. Defendant's practices of disclosing the Private Viewing Information of its customers to Meta continued unabated for the duration of the two-year period preceding the filing of this action.

103. At all times relevant hereto, whenever Plaintiffs or any other person purchased or watched prerecorded video material on Defendant's Website, Defendant disclosed to Meta (*inter alia*) the specific identity of the video material that was requested or obtained (including the URL where such material is hosted), along with the FID of the person who requested or obtained it (which, as discussed above, uniquely identified the person).

104. At all times relevant hereto, whenever Plaintiff or any other person purchased a paid subscription from Defendant on its Website, Defendant disclosed to Meta (*inter alia*) the fact that the person purchased a subscription (including the URL where such a subscription is available for purchase), along with the FID of the person who purchased it (which, as discussed above, uniquely identified the person).

105. At all times relevant hereto, Defendant knew that the Meta Pixel was disclosing its customers' Private Viewing Information to Meta.

106. Although Defendant could easily have programmed its Website so that none of its customers' Private Viewing Information is disclosed to Meta, Defendant instead chose to program its Website so that all of its customers' Private Viewing Information is disclosed to Meta.

107. Before transmitting its customers' Private Viewing Information to Meta, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

108. By intentionally disclosing to Meta Plaintiffs' and its other customers' FIDs together with the identity of the video materials that they each requested or obtained, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

B. Google Analytics

109. Defendant also intentionally discloses Plaintiffs' and its other customers' Private Viewing Information to Google by installing and maintaining a Google Analytics tracking pixel on the Website.

110. When a subscriber watches a prerecorded video on the Website, Defendant discloses to Google, through the operation of the Google Analytics tracking pixel, the user's (i) hashed e-mail address, (ii) Google Analytics client ID,

and (iii) the title, unique numerical identifier, and URL of the video the user is watching.

111. An email address is a personally identifying string of characters which designate an electronic mailbox. Any ordinary person can use an e-mail address to uniquely identity the individual to whom it belongs. Voluminous services exist which enable individuals to look up the owners of a particular email address.

112. A "hash" is an algorithm used to create a digital summary, or fingerprint, of the input. However, the Federal Trade Commission has warned companies for over a decade that hashing is an insufficient method of anonymizing information, including as recently as July 24, 2024.[24] Thus, even in hashed form, email addresses are traceable to individuals.

113. Furthermore, Defendant transmits the user's Google Analytics client ID to Google via the tracking pixel.

114. As with the Meta Pixel, Defendant transmits this personally identifying information to Google along with information identifying each individual video a subscriber obtained or requested, including the video's name, the URL of the webpage hosting the video, and the video's unique numerical identifier.

[24] Ed Felten, *Does Hashing Make Data "Anonymous"?*, Federal Trade Commission (Apr. 22, 2012), available at https://www.ftc.gov/policy/advocacy-research/tech-atftc/2012/04/does-hashing-make-data-anonymous; Federal Trade Commission, *No, Hashing Still Doesn't Making Your Data Anonymous* (July 24, 2024), available at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous.

C. Yahoo Dot

115. Defendant also intentionally discloses Plaintiffs' and its other customers' Private Viewing Information to Yahoo by installing and maintaining a Yahoo Dot tracking pixel on the Website.

116. When a subscriber watches a prerecorded video on the Website, Defendant discloses toYahoo, through the operation of the Yahoo Dot tracking pixel, the user's (i) hashed e-mail address and (ii) the title, unique numerical identifier, and URL of the video the user is watching.

117. An email address is a personally identifying string of characters which designate an electronic mailbox. Any ordinary person can use an e-mail address to uniquely identity the individual to whom it belongs. Voluminous services exist which enable individuals to look up the owners of a particular email address.

118. A "hash" is an algorithm used to create a digital summary, or fingerprint, of the input. However, the Federal Trade Commission has warned companies for over a decade that hashing is an insufficient method of anonymizing information, including as recently as July 24, 2024.[25] Thus, even in hashed form, email addresses are traceable to individuals.

[25] Ed Felten, *Does Hashing Make Data "Anonymous"?*, Federal Trade Commission (Apr. 22, 2012), available at https://www.ftc.gov/policy/advocacy-research/tech-atftc/2012/04/does-hashing-make-data-anonymous; Federal Trade Commission, *No, Hashing Still Doesn't Making Your Data Anonymous* (July 24, 2024), available at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous.

119. As with the Meta Pixel and the Google Analytics Pixel, Defendant transmits this personally identifying information to Yahoo along with information identifying each individual video a subscriber obtained or requested, including the video's name, the URL of the webpage hosting the video, and the video's unique numerical identifier.

CLASS ACTION ALLEGATIONS

120. Plaintiffs seek to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action who subscribed to the Website (www.cowboychannelplus.com) and had their personally identifiable information transmitted to a third party.

121. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

122. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to (a) whether Defendant embedded tracking pixels on its Website that monitor and track actions taken by visitors to its Website; (b) whether Defendant reports the actions and information of visitors to third

parties; (c) whether Defendant knowingly disclosed Plaintiffs' and the Class members' Private Viewing Information to third parties; (d) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; and (e) whether Plaintiffs and Class members are entitled to a statutory damage award of $2,500, as provided by the VPPA.

123. The named Plaintiffs' claims are typical of the claims of the Class in that the Defendant's conduct toward the putative class is the same. That is, Defendant embedded tracking pixels on its Website to monitor and track actions taken by class members to its Website and report this to third parties. Further, the named Plaintiffs and the Class members suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Private Viewing Information to third parties.

124. Plaintiffs are adequate representatives of the Class because they are interested in the litigation; their interests do not conflict with those of the Class members they seek to represent; they have retained competent counsel experienced in prosecuting class actions and intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of all Class members.

125. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class member

may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication of the common questions of law and fact, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION
Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

126. Plaintiffs repeat the allegations asserted in the preceding paragraphs as if fully set forth herein.

127. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

128. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce,

of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

129. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiffs and each of the Class members are a "consumer" within the meaning of the VPPA because they each purchased a subscription to access prerecorded video material or purchased prerecorded video material from Defendant's Website that was sold and delivered to them by Defendant.

130. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The Private Viewing Information that Defendant transmitted to third parties constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because it identifies Plaintiffs and the Class members to third parties as individuals who purchased, and thus "requested or obtained," specific prerecorded video material or a subscription to access prerecorded video material from Defendant via its Website.

131. Defendant knowingly disclosed Plaintiffs' and the Class members' Private Viewing Information to third parties via tracking pixel technology because Defendant intentionally installed and programmed the tracking pixel code on its

Website, knowing that such code would transmit to third parties the identities of the video materials watched by its customers coupled with its customers' unique identifiers (including FIDs).

132. Each of the Plaintiffs could be publicly identified through the use of their FID at the time they requested or obtained prerecorded video materials from Defendant by linking their FIDs to their Facebook accounts, which display their names, photographs, and other personally identifying information.

133. Defendant further knowingly disclosed Plaintiffs' and Class members' Private Viewing Information to third parties via the pixel tracking technology because Defendant intentionally installed and programmed the pixel tracking code on its Website, knowing that such code would transmit to third parties the subscriptions purchased and the specific prerecorded video material requested or obtained by its customers coupled with its customers' unique identifiers (including FIDs).

134. Defendant failed to obtain informed written consent from Plaintiffs or any of the Class members authorizing it to disclose their Private Viewing Information to any third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who purchased prerecorded video material on its Website (including Plaintiff or any of the Class members) informed, written consent that was given in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time,

not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

135. By disclosing Plaintiffs' and Class members' Private Viewing Information, Defendant violated their statutorily protected right to privacy in their Private Viewing Information.

136. Consequently, Defendant is liable to Plaintiff and each of the Class members for damages in the statutorily set sum of $2,500. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendant Rural Media Group, Inc. as follows:

a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

b) For an order declaring that Defendant's conduct as described herein violated the VPPA;

c) For an order finding in favor of Plaintiffs and the Class and against Defendant on all counts asserted herein;

d) For an award of $2,500.00 to Plaintiffs and each of the Class members, as provided by 18 U.S.C. § 2710(c);

e) For an order permanently enjoining Defendant from disclosing the Private Viewing Information of its subscribers to third parties in violation of the VPPA;

f) For prejudgment interest on all amounts awarded; and

g) For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiffs and the Class under Rule 23 and 18 U.S.C. § 2710(c).

Respectfully submitted,

Dated: October 18, 2024

/s/ *Patrick Arnold*

Patrick M. W. Arnold
Texas State Bar No. 24109596
WALLS LANDRY BAKER & OLIVER, PLLC
5910 North Central Expressway, Ste 1560
Dallas, Texas 75206
Telephone: (214) 265-1231
Facsimile: (972) 280-7634
parnold@wlbofirm.com

Tyler K. Somes
Attorney in Charge
District of Columbia Bar No. 90013925
Texas State Bar No. 24110385
HEDIN LLP
1100 15th Street NW, Ste 04-108
Washington, D.C. 20005
Telephone: (202) 900-3332
Facsimile: (305) 200-8801

tsomes@hedinllp.com

Counsel for Plaintiffs and Putative Class